Lyndon-Shirshov basis and anti-commutative algebras*

L. A. Bokut†
School of Mathematical Sciences, South China Normal University
Guangzhou 510631, P. R. China
Sobolev Institute of Mathematics, Russian Academy of Sciences
Siberian Branch, Novosibirsk 630090, Russia
Email: bokut@math.nsc.ru

Yuqun Chen‡ and Yu Li
School of Mathematical Sciences, South China Normal University
Guangzhou 510631, P. R. China
Email: yqchen@scnu.edu.cn
LiYu820615@126.com

Abstract: Chen, Fox, Lyndon 1958 [10] and Shirshov 1958 [29] introduced non-associative Lyndon-Shirshov words and proved that they form a linear basis of a free Lie algebra, independently. In this paper we give another approach to definition of Lyndon-Shirshov basis, i.e., we find an anti-commutative Gröbner-Shirshov basis S of a free Lie algebra such that $Irr(S)$ is the set of all non-associative Lyndon-Shirshov words, where $Irr(S)$ is the set of all monomials of $N(X)$, a basis of the free anti-commutative algebra on X, not containing maximal monomials of polynomials from S. Following from Shirshov's anti-commutative Gröbner-Shirshov bases theory [32], the set $Irr(S)$ is a linear basis of a free Lie algebra.

Key words: Lie algebra, anti-commutative algebra, Lyndon-Shirshov words, Gröbner-Shirshov basis

AMS 2000 Subject Classification: 16S15, 13P10, 17Bxx

1 Introduction

The first linear basis of a free Lie algebra $Lie(X)$ had been given by M. Hall 1950 [14]. He proved that P. Hall long commutators 1933 [15] form a linear basis of the algebra.

*Supported by the NNSF of China (Nos. 11171118; 10911120389) and the NSF of Guangdong Province (No. S2011010003374).

†Supported by RFBR 09-01-00157, LSS–3669.2010.1 and SB RAS Integration grant No. 2009.97 (Russia) and Federal Target Grant Scientific and educational personnel of innovation Russia for 2009-2013 (government contract No. 02.740.11.5191).

‡Corresponding author.

Let us remind that P. Hall (non-associative) monomials are $x_i \in X, x_i > x_j$ if $i > j$, and then, by induction on degree (length), in $((u)(v))$ both (u) and (v) are Hall monomials with $(u) > (v)$, and in $(((u_1)(u_2))(v))$ it must be $(u_2) \leq (v)$. He used a deg-ordering of monomials - monomial of greater degree is greater. In what follow "monomial" would mean "non-associative monomial" ("non-associative word" in Kurosh's terminology [17], adopted by Shirshov, see [34]).

A.I. Shirshov in his Candidate Science Thesis 1953 [27], published in 1962 [31] (it was the first issue of a new Malcev's Journal "Algebra and Logic"), generalized this result and found a series of bases of $Lie(X)$ depending on any ordering of Lie monomials $(u)'$s on X such that $((u_1)(u_2)) > (u_2)$ (it was rediscovered by Viennot 1973 [37], see also 1978 [38]). Any deg-ordering of course satisfies the above condition. Now this series of bases of $Lie(X)$ is called Hall-Shirshov or even Hall bases (the later is used in [24]).

In 1963 [4][1] the first author found another ordering of non-associative monomials with Shirshov's condition and as a result he found a linear basis of $Lie(X)$ compatible with the lower central series of $Lie(X)$ (the result was rediscovered by C. Reutenauer, see his book [24], Ch. 5.3) and even a basis compatible with any polynilpotent series

$$L \supset L^{n_1} \supset (L^{n_1})^{n_2} \supset \dots (\dots((L^{n_1})^{n_2})\dots)^{n_k} \supset \dots, \quad n_i \geq 2.$$

It was a breakthrough in the subject that Shirshov 1958 and Chen-Fox-Lyndon 1958 (in the same year!) found a new basis of $Lie(X)$ now called Lyndon or Lyndon-Shirshov basis. Actually it is an example of the Shirshov's series of bases relative to lex-ordering of monomials: $(u) >_{lex} (v)$ if $u >_{lex} v$ for corresponding (associative) words u, v, otherwise one needs to compare the first monomials of (u), (v), then the second ones. For example, $a > [ab]$, $[a[[ab]b]] > [[a[ab]]b]$. If one starts to construct the Hall-Shirshov basis of $Lie(X)$ using the lex-ordering then one will get Lyndon-Shirshov basis automatically. For example, let $X = \{a, b\}$, $a > b$. Then the first Lyndon-Shirshov monomials are $a, b, [ab], [[ab]b] = [abb], [a[ab]] = [aab], [a[[ab]b]] = [aabb], [a[a[ab]]] = [aaab], [[a[ab][ab]]] = [aabab], [a[a[a[ab]]]] = [aaaab], \dots, [[a[abb]][ab]] = [aabbab], \dots$.

We would see that if $[u]$ is a Lyndon-Shirshov monomial then the underlying word u is a Lyndon-Shirshov word in the sense that $u = vw > wv$ lexicographically for any non-empty words v, w. There is a one to one correspondence between Lyndon-Shirshov monomials and Lyndon-Shirshov words. If u is a Lyndon-Shirshov (LS for short) word then Shirshov 1953 [28] and Lazard 1960 [18] elimination process gives rise to a Lyndon-Shirshov Lie monomial. For example, one has a series of bracketing starting with LS word $aaab$: $aa[ab]$ (join the minimal letter b to the previous one), $a[a[ab]]$ (again join the minimal new "letter" $[ab]$ to the previous letter a), $[a[a[ab]]]$ (again join $[a[ab]]$ to a). At last $[a[a[ab]]]$ is a Lyndon-Shirshov Lie monomial.

Lyndon-Shirshov basis became one of popular bases of free Lie algebras (cf. for example, [8, 24]). One of the main applications of Lyndon-Shirshov basis is the Shirshov's theory of Gröbner-Shirshov bases theory for Lie algebras [33].

Original Shirshov 1958 [29] definition is as follows. Let $X = \{x_i, i = 1, 2, ...\}$ be a totally ordered alphabet, $x_i > x_j$ if $i > j$. A non-empty monomial $u \in X^*$ is called regular ("pravil'noe" in Russian) if $u = vw > wv$ for any non-empty words v, w. Let $<$

[1] Actually, the first author found the result in 1959 but could not published it before Shirshov's one. At last Shirshov said to the first author: "Your result pushes me to publish my result".

be the lexicographical ordering of regular words. A monomial $[u]$ is called regular if (1) the word u is regular, (2) if $[u] = [[v][w]]$, then $[v], [w]$ are regular words, (3) if in (2) $[v] = [[v_1][v_2]]$, then $v_2 \leq w$.

It is easy to see that regular monomials are defined inductively starting with x_i. From condition (2) it follows that $v > w$. From (1)-(3) it easily follows that w is the longest proper regular suffix of u, see [30]. As we explained above, in view of his thesis 1953, the definition of regular words and regular monomials were very natural for Shirshov since he decided to use the lexicographical ordering of monomials and underlying words. Actually Shirshov understood all properties of regular words and monomials by induction on degree using the Lazard-Shirshov elimination process, see, for example, [6].

Standard words ($u = vw < wv$ lexicographically for any non-empty v, w; it is the same as regular word if we invert the ordering on X) were defined by Lyndon 1954 [20].

Original Chen-Fox-Lyndon 1958 [10] definition of the linear basis is (also) based on the notion of standard word and its bracketing $[u] = [[v][w]]$, where w is the longest proper standard suffix of u (then v is automatically standard).

Unfortunately the both Lyndon's and Chen-Fox-Lyndon's papers [10, 20] were unknown to many authors for many years. Many authors, started with 1958, call the basis and words following Shirshov as regular basis and words, see, for example, [1, 2, 5, 12, 13, 16, 21, 22, 23, 36, 39]. We and some authors call them Lyndon-Shirshov words, see, for example, [6, 8, 11].

Many authors, started with 1983, call the words and monomials as Lyndon words and Lyndon basis, see, for example, [19, 24].

It is of some interest to cite some early papers on the matter by M. Schützenberger.

In Schützenberger-Sherman 1963 [25], both the Shirshov 1958 and the Chen-Fox-Lyndon 1958 papers are cited. What is more, they formulated and used a result, Lemma 2, in Shirshov 1958 [29][2] (but they did not claim (!) it is a Chen-Fox-Lyndon 1958 paper result; actually, it is not, see below). The result is sometimes called as "Central result on Lyndon words" (see for example Springer Online, Encyclopedia of Mathematics (edited by Michiel Hazewinkel)).

In Schützenberger 1965 [26], both Chen-Fox-Lyndon 1958 and Shirshov 1958 papers are again cited in according with "Central result on Lyndon words". As it follows from Berstel-Perrin's paper [3][3], actually Schützenberger cited Chen-Fox-Lyndon 1958 paper by a mistake (!).

So to the best of our knowledge the only origin of the "Central result" is Shirshov 1958 paper, at least for Schützenberger and his school.

Some new linear bases of $Lie(X)$ are given in the papers [9, 11, 35].

In this paper we give another approach to definition of LS basis and LS words following Shirshov's (Gröbner-Shirshov bases) theory for anti-commutative algebras [30]. In our

[2]From Schützenberger-Sherman 1963 [25]: "We are indebted to P.M. Cohn for calling our attention to the Shirshov paper. Every $f \in F^+$ has one and only one factorization $f = h_{i_1}h_{i_2}...h_{i_m}$, where h_{i_j} belong to H and satisfy $h_{i_m} \geq \cdots \geq h_{i_2} \geq h_{i_1}$." Here H is the set of Lyndon-Shirshov words in the alphabet F.

[3]From [3]: "A famous theorem concerning Lyndon words asserts that any word w can be factorized in a unique way as a non-increasing product of Lyndon words, i.e., $w = x_1x_2 \ldots x_n$ with $x_1 \geq x_2 \geq \cdots \geq x_n$. This theorem has imprecise origin. It is usually credited to Chen-Fox-Lyndon, following the paper of Schützenberger 1965 [120] in which it appears as an example of factorization of free monoids. Actually, as pointed out to one of us by D. Knuth in 2004 the reference [2] (the Chen, Fox, Lyndon 1958 [10]-L.A. Bokut, Y. Q. Chen, Y. Li) it does not contain explicitly this statement."

previous paper [7] we gave the same kind of results for the Hall basis. To be more precise, in that paper, we had found an anti-commutative Gröbner-Shirshov basis of a free anti-commutative (non-associative) algebra $AC(X)$, such that the corresponding irreducible monomials (not containing the maximal monomials of the Gröbner-Shirshov basis) are exactly the Hall monomials.

Here we prove the same kind of results for LS basis of $Lie(X)$. Namely, we find a linear basis $N(X)$ of $AC(X)$ such that the Composition-Diamond lemma is valid for the triple $(AC(X), N(X), \succ)$, where $\succ$ is the deg-lex ordering on $N(X)$. So Gröbner-Shirshov bases theory is valid for the triple.

Then we find a Gröbner-Shirshov basis of the ideal $J(X)$ of $AC(X)$ generated by all Jacobians $J(N(X), N(X), N(X))$ on $N(X)$. We do it in two steps. First we prove that the irreducible set of monomials from $N(X)$ relative to $J(N(X), N(X), N(X))$ is exactly the set of Lyndon-Shirshov monomials. It gives a new approach to LS monomials. By the way, we also prove that for any monomial $(u) \in N(X)$ its associative support u has a form v^m, where v is a LS word. In some sense it gives a new approach to LS words.

Our next step is the main result of the paper (see Theorem 4.6):

Let $(AC(X), N(X), \succ, J(X))$ be as above. Then the set $J(LS(X), LS(X), LS(X))$ of all Jacobians on LS monomials is a Gröbner-Shirshov basis of the ideal $J(X)$. What is more, $Irr(J(LS(X), LS(X), LS(X)))$, the set of all monomials of $N(X)$ not containing maximal monomials of polynomials from $J(LS(X), LS(X), LS(X))$, is exactly the set of all LS monomials. Hence, the later is a linear basis of the free Lie algebra $Lie(X)$.

For completeness we formulate Composition-Diamond lemma for the triple $(AC(X), N(X), \succ)$. The proof is essentially the same as in [29] and [7] in which the difference is that now $N(X)$ and the ordering are different from those papers.

2 A basis of a free anti-commutative algebra AC(X)

Let X be a well-ordered set, X^* the set of all associative words, X^{**} the set of all nonassociative words, $>_{lex}$, $>_{dex-lex}$ the lexicographical ordering and the degree lexicographical ordering on X^* respectively.

Let (u) be a nonassociative word on X and denote $|(u)|$ the degree of (u), the number of the letters occur in (u).

An ordering $\succ_{lex}$ on X^{**} is inductively defined by: $((u_1)(u_2)) \succ_{lex} ((v_1)(v_2))$ if and only if one of the following cases holds

(a) $u_1u_2 >_{lex} v_1v_2$,

(b) $u_1u_2 = v_1v_2$ and $(u_1) \succ_{lex} (v_1)$,

(c) $u_1u_2 = v_1v_2$, $(u_1) = (v_1)$ and $(u_2) \succ_{lex} (v_2)$.

We define normal words $(u) \in X^{**}$ by induction on $|(u)|$:

(i) $x_i \in X$ is a normal word.

(ii) $(u) = ((u_1)(u_2))$ is normal if both (u_1) and (u_2) are normal and $(u_1) \succ_{lex} (u_2)$.

Denote (u) by $[u]$, if (u) is normal.

Before we discuss some combinatorial properties of normal words on X, we need to cite the definition of associative LS words and some important properties of associative LS words.

An associative word u is an associative LS word (ALSW for short) if, for arbitrary nonempty v and w such that $u = vw$, we have $u >_{lex} wv$.

We will use the following properties of ALSWs (see [6]):

1. if $u = vw$ is an ALSW, where v, w are not empty word, then $u >_{lex} w$;
2. if u, v are ALSWs and $u >_{lex} v$, then uv is also an ALSW;
3. each nonempty word $u \in X^*$ has a unique decomposition:

$$u = u_1 u_2 \ldots u_n,$$

where u_i is an ALSW and $u_1 \leq_{lex} u_2 \leq_{lex} \ldots \leq_{lex} u_n$.

Lemma 2.1 *Let u, v be ALSWs and $u >_{lex} v$. Then $u^m >_{lex} v^n$ for any $m, n \geq 1$.*

Proof. If $u = x_1 \cdots x_t y \cdots$ and $v = x_1 \cdots x_t z \cdots$, where $y >_{lex} z$, then $u^m >_{lex} v^n$ clearly for any $m, n \geq 1$. Suppose u is a proper prefix of v, i.e., $v = uw$ for some nonempty word w. Then there exists an l such that $v = u^l c$, u is not a prefix of c. If c is empty, then $v = u^l$, which leads to a contradiction by the property 3. This means that c is not empty. Then, by the property 1, $u >_{lex} v >_{lex} c$ and thus $u = x_1 \cdots x_t y \cdots$ and $c = x_1 \cdots x_t z \cdots$, where $t \geq 0$ and $y >_{lex} z$. If this is the case, $u^m >_{lex} v^n$ clearly. $\square$

Lemma 2.2 *Let $[u]$ be a normal word on X. Then $u = w^n$, w is an ALSW and $n \geq 1$.*

Proof. If $[u] = x_i$, then this is a trivial case. Suppose $[u] = [[u_1][u_2]]$. By induction on $|[u]|$, we have $u_1 = w_1^{m_1}$ and $u_2 = w_2^{m_2}$, where w_1, w_2 are ALSWs and $m_1, m_2 \geq 1$. If $w_1 >_{lex} w_2$, then, by the property 1 and the property 2 of ALSWs, $u = w_1^{m_1} w_2^{m_2}$ is an ALSW. If $w_1 = w_2$, then $u = w_1^{m_1+m_2}$. If $w_1 <_{lex} w_2$, then, by Lemma 2.1, $u = w_1^{m_1} <_{lex} v = w_2^{m_2}$ and this contradicts $[u]$ is a normal word. $\square$

Corollary 2.3 *If $[u]$ is normal and $[u] = [[u_1][u_2]]$, then $u_1 u_2 \geq_{lex} u_2 u_1$.*

Let k be a field, $N(X)$ the set of all normal words $[u]$ on X and $AC(X)$ a k-vector space spanned by $N(X)$. Now define the product of normal words by the following way: for any $[u], [v] \in N(X)$,

$$[u][v] = \begin{cases} [[u][v]], & \text{if } [u] \succ_{lex} [v] \\ -[[v][u]], & \text{if } [u] \prec_{lex} [v] \\ 0, & \text{if } [u] = [v] \end{cases}$$

Remark: By definition, for any $(u) \in X^{**}$, there exists a unique $[v] \in N(X)$ such that, in $AC(X)$, $(u) = \pm[v]$ or 0. Now we denote $[v]$ by $\widetilde{(u)}$ if $(u) \neq 0$.

Then we can get the following theorem by a straightforward proof.

Theorem 2.4 *$AC(X)$ is a free anti-commutative algebra generated by X.*

A well ordering $>$ on $N(X)$ is called monomial if it satisfies the following condition:

$$[u] > [v] \Rightarrow \widetilde{([u][w])} > \widetilde{([v][w])}$$

for any $[w] \in N(X)$ such that $[w] \neq [u],\ [w] \neq [v]$.

If $>$ is a monomial ordering on $N(X)$, then we have

$$[u] > [v] \Rightarrow [a[u]b] > \widetilde{(a[v]b)},$$

where $[a[u]b]$ is a normal word with subword $[u]$ and $(a[v]b) = [a[u]b]|_{[u]\mapsto[v]} \neq 0$.

We define an ordering $\succ_{deg-lex}$ on $N(X)$ by: $((u_1)(u_2)) \succ_{deg-lex} ((v_1)(v_2))$ if and only if one of the following cases holds

(a) $u_1u_2 >_{deg-lex} v_1v_2$,

(b) $u_1u_2 = v_1v_2$ and $(u_1) \succ_{deg-lex} (v_1)$,

(c) $u_1u_2 = v_1v_2$, $(u_1) = (v_1)$ and $(u_2) \succ_{deg-lex} (v_2)$.

In this paper, unless another statement, we use the above ordering $\succ_{deg-lex}$ on $N(X)$.

Then we have the following lemmas.

Lemma 2.5 *Suppose that $[u]_\mu$ and $[u]_\nu$ are two different bracketing on a word u such that both $[u]_\mu$ and $[u]_\nu$ are normal words. If $[u]_\mu \succ_{deg-lex} [u]_\nu$, then $[u]_\mu \prec_{lex} [u]_\nu$.*

Proof. Let us consider the basic case $u = x_ix_jx_k, i > j > k$. Then $[u]_\mu \succ_{deg-lex} [u]_\nu$ implies that $[u]_\mu = [[x_ix_j]x_k]$ and $[u]_\nu = [x_i[x_jx_k]]$, and thus $[u]_\mu = [[x_ix_j]x_k] \prec_{lex} [u]_\nu = [x_i[x_jx_k]]$. Suppose that $[u]_\mu = [[u_1]_{\mu_1}[u_2]_{\mu_2}]$ and $[u]_\nu = [[u_1']_{\nu_1}[u_2']_{\nu_2}]$. If $u_1 >_{deg-lex} u_1'$, then u_1' is a proper prefix of u_1 and obviously $[u]_\mu \prec_{lex} [u]_\nu$. If $u_1 = u_1'$ and $[u_1]_{\mu_1} \succ_{deg-lex} [u_1']_{\nu_1}$, then, by induction on $|u|$, $[u_1]_{\mu_1} \prec_{lex} [u_1']_{\nu_1}$ and thus $[u]_\mu \prec_{lex} [u]_\nu$. If $[u_1]_{\mu_1} = [u_1']_{\nu_1}$, then $u_2 = u_2'$ and $[u_2]_{\mu_2} \succ_{deg-lex} [u_2']_{\nu_2}$, and hence we complete our proof by induction on $|u|$. $\square$

Lemma 2.6 *The ordering $\succ_{deg-lex}$ is a monomial well ordering on $N(X)$.*

Proof. It is easy to check that the ordering $\succ_{deg-lex}$ is a well ordering. Suppose that $[u],[v],[w] \in N(X)$, $[u] \succ_{deg-lex} [v]$, $[w] \neq [u]$ and $[w] \neq [v]$. If $|[u]| > |[v]|$, then $\widetilde{[u][w]} \succ_{deg-lex} \widetilde{[v][w]}$ clearly. If $|[u]| = |[v]|$ and $u >_{lex} v$, then we consider the following three cases $w \geq_{lex} u >_{lex} v$, $u >_{lex} w >_{lex} v$ and $u >_{lex} v \geq_{lex} w$. For the cases $w \geq_{lex} u >_{lex} v$ and $u >_{lex} v \geq_{lex} w$, it is obvious that $\widetilde{[u][w]} \succ_{deg-lex} \widetilde{[v][w]}$. For the case $u >_{lex} w >_{lex} v$, $\widetilde{[u][w]} = [[u][w]] \succ_{deg-lex} [[w][v]] = \widetilde{[v][w]}$ since by Corrollary 2.3 we have $uw \geq_{lex} wu >_{lex} wv$. If $u = v >_{lex} w$ or $w >_{lex} u = v$, $\widetilde{[u][w]} \succ_{deg-lex} \widetilde{[v][w]}$ clearly. Suppose that $u = v = w$ and $[u] \succ_{dex-lex} [v] \succ_{dex-lex} [w]$. Then, by Lemma 2.5, $[u] \prec_{lex} [v] \prec_{lex} [w]$ and thus $\widetilde{[u][w]} = [[w][u]] \succ_{deg-lex} [[w][v]] = \widetilde{[v][w]}$. We can similarly check the other two cases $[u] \succ_{dex-lex} [w] \succ_{dex-lex} [v]$ and $[w] \succ_{dex-lex} [u] \succ_{dex-lex} [v]$ to complete our proof. $\square$

3 Composition-Diamond lemma for $AC(X)$

In this section, we formulate Composition-Diamond lemma for the free anti-commutative algebra $AC(X)$.

Given a polynomial $f \in AC(X)$, it has the leading word $[\overline{f}] \in N(X)$ according to the ordering $\succ_{dex-lex}$ on $N(X)$, such that

$$f = \sum_{[u]\in N} f([u])[u] = \alpha[\overline{f}] + \sum \alpha_i[u_i],$$

where $[\overline{f}] \succ_{deg-lex} [u_i],\ \alpha,\ \alpha_i,\ f([u]) \in k$. We call $[\overline{f}]$ the leading term of f. f is called monic if $\alpha = 1$.

Definition 3.1 *Let $S \subset AC(X)$ be a set of monic polynomials, $s \in S$ and $(u) \in X^{**}$. We define S-word $(u)_s$ by induction:*

(i) $(s)_s = s$ is an S-word of S-length 1.

(ii) If $(u)_s$ is an S-word of S-length k and (v) is a nonassociative word of length l, then

$$(u)_s(v) \text{ and } (v)(u)_s$$

are S-words of length $k+l$.

Definition 3.2 *An S-word $(u)_s$ is called a normal S-word, if $(u)_{[\bar{s}]} = (a[\bar{s}]b)$ is a normal word. We denote $(u)_s$ by $[u]_s$ if $(u)_s$ is a normal S-word. We also call the normal S-word $[u]_s$ to be normal s-word. From Lemma 2.5 it follows that $\overline{[u]_s} = [u]_{[\bar{s}]}$.*

Let f, g be monic polynomials in $AC(X)$. Suppose that there exist $a, b \in X^*$ such that $[\bar{f}] = [a[\bar{g}]b]$, where $[agb]$ is a normal g-word. Then we set $[w] = [\bar{f}]$ and define the composition of inclusion

$$(f, g)_{[w]} = f - [agb].$$

We note that $(f, g)_{[w]} \in Id(f, g)$ *and* $\overline{(f, g)_{[w]}} \prec_{deg-lex} [w]$, where $Id(f, g)$ is the ideal of $AC(X)$ generated by f, g.

Transformation $f \mapsto f - [agb]$ is called the Elimination of Leading Word (ELW) of g in f.

Given a nonempty subset $S \subset AC(X)$, we shall say that the composition $(f, g)_{[w]}$ is trivial modulo $(S, [w])$, if

$$(f, g)_{[w]} = \sum_i \alpha_i[a_i s_i b_i],$$

where each $\alpha_i \in k,\ a_i, b_i \in X^*,\ s_i \in S,\ [a_i s_i b_i]$ is normal S-word and $[a_i[\bar{s}_i]b_i] \prec_{deg-lex} [w]$. If this is the case, then we write $(f, g)_{[w]} \equiv 0\ mod(S, [w])$.

Let us note that if $(f, g)_{[w]}$ goes to 0 by ELW's of S, then $(f, g)_{[w]} \equiv 0 \text{ mod}(S, [w])$. Indeed, using ELW's of S, we have

$$(f, g)_{[w]} \mapsto (f, g)_{[w]} - \alpha_1[a_1 s_1 b_1] = f_2 \mapsto f_2 - \alpha_2[a_2 s_2 b_2] \mapsto \cdots \mapsto 0.$$

So, $(f,g)_{[w]} = \sum_i \alpha_i[a_i s_i b_i]$, where $[a_i[\bar{s_i}]b_i] \preceq_{deg-lex} \overline{(f,g)_{[w]}} \prec_{deg-lex} [w]$.

In general, for $p, q \in AC(X)$, we write

$$p \equiv q \quad mod(S, [w])$$

which means that $p - q = \sum \alpha_i[a_i s_i b_i]$, where each $\alpha_i \in k$, $a_i, b_i \in X^*$, $s_i \in S$ and $[a_i[\bar{s_i}]b_i] \prec_{deg-lex} [w]$.

Definition 3.3 *Let $S \subset AC(X)$ be a nonempty set of monic polynomials and the ordering $\succ_{deg-lex}$ on $N(X)$ as before. Then the set S is called a Gröbner-Shirshov basis (GSB for short) if any composition $(f,g)_{[w]}$ with $f, g \in S$ is trivial modulo $(S, [w])$, i.e., $(f,g)_{[w]} \equiv 0$ $mod(S, [w])$.*

Lemma 3.4 *Let $S \subset AC(X)$ be a nonempty set of monic polynomials and $Irr(S) = \{[u] \in N(X) | [u] \neq [a[\bar{s}]b]\ a, b \in X^*,\ s \in S$ and $[asb]$ is a normal S-word$\}$. Then for any $f \in AC(X)$,*

$$f = \sum_{[u_i] \preceq_{deg-lex} [\bar{f}]} \alpha_i [u_i] + \sum_{[a_j[\overline{s_j}]b_j] \preceq_{deg-lex} [\bar{f}]} \beta_j [a_j s_j b_j],$$

where each $\alpha_i, \beta_j \in k$, $[u_i] \in Irr(S)$ and $[a_j s_j b_j]$ normal S-word.

By a similar proof to the Theorem 3.10 in [7], we have the following theorem. Here the difference is that now $N(X)$ and the ordering are different from [7]. We omit the detail.

Theorem 3.5 *Let $S \subset AC(X)$ be a nonempty set of monic polynomials, the ordering $\succ_{deg-lex}$ on $N(X)$ as before and $Id(S)$ the ideal of $AC(X)$ generated by S. Then the following statements are equivalent:*

(i) S is a Gröbner-Shirshov basis.

(ii) $f \in Id(S) \Rightarrow [\bar{f}] = [a[\bar{s}]b]$ for some $s \in S$ and $a, b \in X^*$, where $[asb]$ is a normal S-word.

(iii) $Irr(S) = \{[u] \in N(X) | [u] \neq [a[\bar{s}]b]\ a, b \in X^*,\ s \in S$ and $[asb]$ is a normal S-word$\}$ is a linear basis of the algebra $AC(X|S) = AC(X)/Id(S)$.

4 Gröbner-Shirshov basis for a free Lie algebra

In this section, we give a new approach to non-associative Lyndon-Shirshov words. We represent the free Lie algebra by the free anti-commutative algebra and give a Gröbner-Shirshov basis for the free Lie algebra.

The proof of the following theorem is straightforward and we omit the detail.

Theorem 4.1 *Let $AC(X)$ be the free anti-commutative algebra and let*

$$S = \{([u][v])[w] - ([u][w])[v] - [u]([v][w]) \mid [u], [v], [w] \in N(X) \text{ and } [u] \succ_{lex} [v] \succ_{lex} [w]\}.$$

Then the algebra $AC(X|S)$ is the free Lie algebra generated by X. $\square$

We now cite the definition of non-associative Lyndon-Shirshov words (NLSWs) given by induction on length:

1) x is a NLSW for any $x \in X$,

2) a non-associative word $((v)(w))$ is called a NLSW if

   (a) both (v) and (w) are NLSWs, and $v >_{lex} w$,

   (b) if $(v) = ((v_1)(v_2))$, then $v_2 \leq_{lex} w$.

Note that each NLSW (u) is a normal word. We denote (u) by $[[u]]$ if (u) is a NLSW.

There are some known properties of NLSW (see [6]):

(1) for any NLSW $[[u]]$, u is an ALSW;

(2) for each ALSW u, there exists a unique bracketing (u) on u such that (u) is a NLSW. It follows that $[[u]] \succ_{lex} [[v]]$ iff $u >_{lex} v$.

In general, we don't know what is the leading term of a polynomial in S. However, for some special polynomials, we know exactly the leading terms of them, which can help us to study the ideal generated by S.

Lemma 4.2 *Let $[[u]], [[v]], [[w]]$ be NLSWs and $[[u]] \succ_{lex} [[v]] \succ_{lex} [[w]]$. Denote f_{uvw} the polynomial $([[u]][[v]])[[w]] - ([[u]][[w]])[[v]] - [[u]]([[v]][[w]])$. Then $\overline{f_{uvw}} = ([[u]][[v]])[[w]]$.*

Proof. Following from $[[u]] \succ_{lex} [[v]] \succ_{lex} [[w]]$, we get $u >_{lex} v >_{lex} w$. Then $([[u]][[v]])[[w]] = ([[u]][[v]])[[w]]$ (for $u >_{lex} uv >_{lex} v >_{lex} w$) and $[[u]]([[v]][[w]]) = [[u]]([[v]][[w]])$ (for $u >_{lex} v >_{lex} vw >_{lex} w$). $(([[u]][[w]])[[v]]$ may be $([[u]][[w]])[[v]]$ or $[[v]]([[u]][[w]])$, however, we have $uvw > uwv, vuw$ and thus $\overline{f_{uvw}} = ([[u]][[v]])[[w]]$. $\square$

The following theorem gives us a new approach to NLSWs.

Theorem 4.3 *Let T be the set consisting of all NLSWs. Then*

$$Irr(S) = T.$$

Proof. Suppose $[u] \in Irr(S)$. We will show that $[u]$ is a NLSW by induction on $|[u]| = n$. If $n = 1$, then $[u] = x \in X$ which is already a NLSW. Let $n > 1$ and $[u] = [[v][w]]$. By induction, we have that $[v], [w]$ are NLSWs. If $|v| = 1$, then $[u]$ is a NLSW. If $|[v]| > 1$ *and* $[v] = [[v_1][v_2]]$, then $v_2 \leq_{lex} w$ because of Lemma 4.2 and $[u] \in Irr(S)$. So, $[u]$ is a NLSW.

It's clear that every NLSW is in $Irr(S)$ since every subword of NLSW is also a NLSW. $\square$

In order to prove that S is a GSB in $AC(X)$, we consider the subset of S:

$$\begin{aligned} S_0 \;=\; & \{([[u]][[v]])[[w]] - ([[u]][[w]])[[v]] - [[u]]([[v]][[w]]) \mid \\ & [[u]] \succ_{lex} [[v]] \succ_{lex} [[w]],\ and\ [[u]], [[v]], [[w]]\ are\ NLSWs\}. \end{aligned}$$

In the following, we prove that S_0 generates the same ideal as S, and S_0 is a GSB in $AC(X)$, which implies that S is also a GSB.

According to Lemma 3.4 and $Irr(S_0) = T$ (similar proof to Theorem 4.3), we get the following lemma.

Lemma 4.4 *In $AC(X)$, any normal word $[u]$ has the following presentation:*

$$[u] = \sum_i \alpha_i [[u_i]] + \sum_j \beta_j [u_j]_{s_j},$$

where $\alpha_i, \beta_j \in k$, $[[u_i]]$ are NLSWs, $[u_j]_{s_j}$ normal S_0-words, $s_j \in S_0$, $[[u_i]], [u_j]_{[\overline{s_j}]} \preceq_{deg-lex} [u]$. Moreover, each $[[u_i]]$ has the same degree as $[u]$.

Lemma 4.5 *Suppose S and S_0 are sets defined as before. Then, in $AC(X)$, we have*

$$Id(S) = Id(S_0).$$

Proof. Since S_0 is a subset of S, it suffices to prove that $AC(X|S_0)$ is a Lie algebra. We need only to prove that, in $AC(X|S_0)$,

$$([u][v])[w] - ([u][w])[v] - [u]([v][w]) = 0,$$

where $[u], [v], [w] \in N(X)$. By Lemma 4.4, it suffices to prove

$$([[u]][[v]])[[w]] - ([[u]][[w]])[[v]] - [[u]]([[v]][[w]]) = 0,$$

where $[[u]] \succ_{lex} [[v]] \succ_{lex} [[w]]$. This is trivial by the definition of S_0. $\square$

Theorem 4.6 *Let*

$$S_0 = \{([[u]][[v]])[[w]] - ([[u]][[w]])[[v]] - [[u]]([[v]][[w]]) \mid [[u]] \succ_{lex} [[v]] \succ_{lex} [[w]], \text{ and } [[u]], [[v]], [[w]] \text{ are nonassociative LS words} \}.$$

Then the set S_0 is a Gröbner-Shirshov basis in $AC(X)$.

Proof. To simplify notations, we write $\hat{u}$ for $[[u]]$ and $\hat{u}_1\hat{u}_2\cdots\hat{u}_n$ for $((((\hat{u}_1)\hat{u}_2)\cdots)\hat{u}_n)$. Let $f_{uvw} = \hat{u}\hat{v}\hat{w} - \hat{u}\hat{w}\hat{v} - \hat{u}(\hat{v}\hat{w})$, where $\hat{u}, \hat{v}, \hat{w}$ are NLSWs and $u >_{lex} v >_{lex} w$. We know $\overline{f_{uvw}} = \hat{u}\hat{v}\hat{w}$ from Lemma 4.2.

Suppose $\overline{f_{u_1v_1w_1}}$ is a subword of $\overline{f_{uvw}}$. Since $\hat{u}, \hat{v}, \hat{w}$ are NLSWs, we have $\hat{u}_1\hat{v}_1\hat{w}_1 = \hat{u}\hat{v}, \hat{u} = \hat{u}_1\hat{v}_1$ and $\hat{v} = \hat{w}_1$. We will prove that the composition

$$(f_{uvw}, f_{u_1v_1w_1})_{\hat{u}\hat{v}\hat{w}}$$

is trivial modulo $(S_0, \hat{u}\hat{v}\hat{w})$. We note that $u_1 >_{lex} v_1 >_{lex} w_1 = v >_{lex} w$.

Firstly, we prove that the following statements hold mod$(S_0, \hat{u}\hat{v}\hat{w})$:

1) $\hat{u}_1\hat{v}\hat{v}_1\hat{w} - \hat{u}_1\hat{v}\hat{w}\hat{v}_1 - \hat{u}_1\hat{v}(\hat{v}_1\hat{w}) \equiv 0.$

2) $\hat{u}_1(\hat{v}_1\hat{v})\hat{w} - \hat{u}_1\hat{w}(\hat{v}_1\hat{v}) - \hat{u}_1(\hat{v}_1\hat{v}\hat{w}) \equiv 0.$

3) $\hat{u}_1\hat{w}\hat{v}_1\hat{v} - \hat{u}_1\hat{w}\hat{v}\hat{v}_1 - \hat{u}_1\hat{w}(\hat{v}_1\hat{v}) \equiv 0.$

4) $\hat{u}_1(\hat{v}_1\hat{w})\hat{v} - \hat{u}_1\hat{v}(\hat{v}_1\hat{w}) - \hat{u}_1(\hat{v}_1\hat{w}\hat{v}) \equiv 0.$

5) $\hat{u}_1(\hat{v}\hat{w})\hat{v}_1 - \hat{u}_1(\hat{v}\hat{w}\hat{v}_1) - \hat{u}_1\hat{v}_1(\hat{v}\hat{w}) \equiv 0.$

6) $\hat{u}_1\hat{v}\hat{w}\hat{v}_1 - \hat{u}_1\hat{w}\hat{v}\hat{v}_1 - \hat{u}_1(\hat{v}\hat{w})\hat{v}_1 \equiv 0.$

7) $\hat{u}_1\hat{v}_1\hat{w}\hat{v} - \hat{u}_1\hat{w}\hat{v}_1\hat{v} - \hat{u}_1(\hat{v}_1\hat{w})\hat{v} \equiv 0.$

8) $\hat{u}_1(\hat{v}_1\hat{v}\hat{w}) - \hat{u}_1(\hat{v}_1\hat{w}\hat{v}) - \hat{u}_1(\hat{v}_1(\hat{v}\hat{w})) \equiv 0.$

We only prove 1). 2)–5) are similarly proved to 1) and 6)–8) follow from ELW's of S_0.

By ELW's of S_0, we may assume, without loss of generality, that $\hat{u}_1\hat{v}$ is a NLSW. If $u_1v >_{lex} v_1$, then $\hat{u}_1\hat{v}\hat{v}_1\hat{w} - \hat{u}_1\hat{v}\hat{w}\hat{v}_1 - \hat{u}_1\hat{v}(\hat{v}_1\hat{w}) = f_{(u_1v)v_1w} \equiv 0$. If $u_1v = v_1$, then $\hat{u}_1\hat{v}\hat{v}_1\hat{w} - \hat{u}_1\hat{v}\hat{w}\hat{v}_1 - \hat{u}_1\hat{v}(\hat{v}_1\hat{w}) = 0$. If $u_1v <_{lex} v_1$, then $\hat{u}_1\hat{v}\hat{v}_1\hat{w} - \hat{u}_1\hat{v}\hat{w}\hat{v}_1 - \hat{u}_1\hat{v}(\hat{v}_1\hat{w}) = -f_{v_1(u_1v)w} \equiv 0$.

Secondly, we have

$$\begin{aligned}(f_{uvw}, f_{u_1v_1w_1})_{\hat{u}\hat{v}\hat{w}} &= f_{uvw} - (f_{u_1v_1w_1})\hat{w} \\ &= \hat{u}_1\hat{v}\hat{v}_1\hat{w} + \hat{u}_1(\hat{v}_1\hat{v})\hat{w} - \hat{u}_1\hat{v}_1\hat{w}\hat{v} - \hat{u}_1\hat{v}_1(\hat{v}\hat{w}).\end{aligned}$$

Let

$$A = \hat{u}_1\hat{v}\hat{v}_1\hat{w} + \hat{u}_1(\hat{v}_1\hat{v})\hat{w} \quad and \quad B = -\hat{u}_1\hat{v}_1\hat{w}\hat{v} - \hat{u}_1\hat{v}_1(\hat{v}\hat{w}).$$

Then, by 1)–8), we have

$$\begin{aligned}A &\equiv \hat{u}_1\hat{v}\hat{w}\hat{v}_1 + \hat{u}_1\hat{v}(\hat{v}_1\hat{w}) + \hat{u}_1\hat{w}(\hat{v}_1\hat{v}) + \hat{u}_1(\hat{v}_1\hat{v}\hat{w}) \\ &\equiv \hat{u}_1\hat{w}\hat{v}\hat{v}_1 + \hat{u}_1(\hat{v}\hat{w})\hat{v}_1 + \hat{u}_1\hat{v}(\hat{v}_1\hat{w}) + \hat{u}_1\hat{w}(\hat{v}_1\hat{v}) + \hat{u}_1(\hat{v}_1\hat{w}\hat{v}) + \hat{u}_1(\hat{v}_1(\hat{v}\hat{w}))\end{aligned}$$

and

$$\begin{aligned}-B &= \hat{u}_1\hat{v}_1\hat{w}\hat{v} + (\hat{u}_1\hat{v}_1)(\hat{v}\hat{w}) \\ &\equiv \hat{u}_1\hat{w}\hat{v}_1\hat{v} + \hat{u}_1(\hat{v}_1\hat{w})\hat{v} + \hat{u}_1\hat{v}_1(\hat{v}\hat{w}) \\ &\equiv \hat{u}_1\hat{w}\hat{v}\hat{v}_1 + \hat{u}_1\hat{w}(\hat{v}_1\hat{v}) + \hat{u}_1\hat{v}(\hat{v}_1\hat{w}) + \hat{u}_1(\hat{v}_1\hat{w}\hat{v}) + \hat{u}_1\hat{v}_1(\hat{v}\hat{w}).\end{aligned}$$

So,

$$(f_{uvw}, f_{u_1v_1w_1})_{\hat{u}\hat{v}\hat{w}} = A + B \equiv \hat{u}_1(\hat{v}\hat{w})\hat{v}_1 + \hat{u}_1(\hat{v}_1(\hat{v}\hat{w})) - \hat{u}_1\hat{v}_1(\hat{v}\hat{w}) \equiv 0 \quad mod(S_0, \hat{u}\hat{v}\hat{w}).$$

This completes our proof. □

References

[1] Y.A. Bahturin, A.A. Mikhalev, V.M. Petrogradskij, M.V. Zajtsev, Infinite dimensional Lie superalgebras, De Gruyter Expositions in Mathematics. 7. Berlin etc.: W. de Gruyter. x, 250 p. (1992).

[2] Y.A. Bahturin, A. Olshanskii, Filtrations and distortion in infinite dimensional algebras, J. Algebra 327 (1) (2011) 251-291.

[3] J. Berstel, D. Perrin, The origins of combinatorics on words, Eur. J. Comb. 28 (3) (2007) 996-1022.

[4] L.A. Bokut, Bases of free polynilpotent Lie agebras, Algebra i Logika 2 (4) (1963) 13-20.

[5] L.A. Bokut, Insolvability of the word problem for Lie algebras, and subalgebras of finitely presented Lie algebras, Izvestija AN USSR (mathem.) 36 (6)(1972) 1173-1219.

[6] L.A. Bokut, Y.Q. Chen, Gröbner-Shirshov bases for Lie algebras: after A. I. Shirshov, Southeast Asian Bull. Math. 31 (6) (2007) 1057-1076.

[7] L.A. Bokut, Y.Q. Chen, Y. Li, Anti-commuatative Gröbner-Shirshov basis of free Lie algebra, Science in China 52 (2) (2009) 244-253.

[8] L.A. Bokut, G.P. Kukin, Algorithmic and combinatorial algebra, (English) [B] Mathematics and its Applications (Dordrecht), 255. Dordrecht: Kluwer Academic Publishers. xvi, 384 p. (1994).

[9] R.M. Bryant, L.G. Kovach, R. Stöhr, Invariant bases for free Lie rings, Q. J. Math. 53 (2002) 1-17.

[10] K.-T. Chen, R.H. Fox, R.C. Lyndon, Free differential calculus. IV. The quotient groups of the lower central series, Ann. Math. 68 (2) (1958) 81-95.

[11] E.S. Chibrikov, A right normed basis for free Lie algebras and Lyndon-Shirshov words, J. Algebra 302 (2006) 593-612.

[12] P.M. Cohn, Universal algebra, Harper's Series in Modern Mathematics, New York-Evanston-London: Harper and Row, Publishers 1965, XV, 333 p. (1965).

[13] P.M. Cohn, Universal algebra, (Russian). Moskau: Verlag 'Mir'. 352 p. (1968). A.G. Kurosh (Ed).

[14] M. Hall, A basis of free Lie rings and higher commutators in free groups, Proc. Amer. Math. Soc. 1 (1950) 575-581.

[15] P. Hall, A contribution to the theory of groups of prime power order, Proc. London Math. Soc. Ser. 2 (64) (1933) 29-95.

[16] V.K. Kharchenko, PBW-bases of coideal subalgebras and a freeness theorem, Trans. Amer. Math. Soc. 360 (10) (2008) 5121-5143.

[17] A. Kurosh, Nonassociative free algebras and free products of algebras, Mat. Sb. N. Ser. 20 (62) (1947) 239-262.

[18] M. Lazard, Groupes, anneaux de Lie et probleme de Burnside. C.I.M.E., Gruppi, Anelli di Lie e Theoria della Coomologia, 60 p. (1960).

[19] M. Lothaire, (D. Perrin, C. Reutenauer, J. Berstel, J.E. Pin, G. Pirillo, D. Foata, J. Sakarovitch, I. Simon, M.P. Schützenberger, C. Choffrut, R. Cori, R. Lyndon, G.-C. Rota). Combinatorics on words. Foreword by Roger Lyndon. (English) Encyclopedia of Mathematics and Its Applications, Vol. 17. Reading, Massachusetts, etc.: Addison-Wesley Publishing Company, Advanced Book Program/World Science Division. XIX, 238 p. (1983).

[20] R.C. Lyndon, On Burnside's problem, Trans. Amer. Math. Soc. 77 (1954) 202-215.

[21] A.A. Mikhalev, The composition lemma for color Lie superalgebras and for Lie p-superalgebras, (English) Algebra, Proc. Int. Conf. Memory A.I. Mal'cev, Novosibirsk/USSR 1989, Contemp. Math. 131, Pt. 2, (1992) 91-104.

[22] Y.P. Razmyslov, Identities of algebras and their representations, (Tozhdestva algebr i ikh predstavlenija.) (Russian. English summary) Sovremennaya Algebra, 14. Moskva: Nauka. 432 p. R. 5.20 (1989).

[23] Y.P. Razmyslov, Identities of algebras and their representations, Transl. from the Russian by A. M. Shtern. Transl. ed. by Simeon Ivanov. Translations of Mathematical Monographs. 138. Providence, RI: American Mathematical Society (AMS). xiii, 318 p. (1994).

[24] C. Reutenauer, Free Lie algebras, Oxford Science Publications, 1993.

[25] M.P. Schützenberger, S. Sherman, On a formal product over the conjugate classes in a free group, J. Math. Anal. Appl. 7 (1963) 482-488. From the review MR0158002 (28 #1230) "The present paper gives a direct proof of the above identity by a technique resembling A.I. Shirshov's construction of basis commutators [A.I. Shirshov, Mat. Sb. (N.S.) 45 (87) (1958) 113-122; MR0099356 (20 #5796)]" P.M. Cohn

[26] M.P. Schützenberger, On a factorization of free monoids, Proc. Amer. Math. Soc. 16 (1965) 21-24.

[27] A.I. Shirshov, Some problems in the theory of non-associative rings and algebras, Candidate of Science Thesis, Moscow State University, 1953. see http://math.nsc.ru/LBRT/a1/ShirshovPhD.djvu and http://202.116.32.252/Article_Show.asp?ArticleID=3187

[28] A.I. Shirshov, Subalgebras of free Lie algebras, Mat. Sb. 33 (75) (1953) 441-452.

[29] A.I. Shirshov, On free Lie rings, *Mat. Sb.* 45 (2) (1958) 113–122.

[30] A.I. Shirshov, Some problems in the theory of rings that are nearly associative, Uspekhi Mat. Nauk. 13 (1958), no. 6 (84), 3-20.

[31] A.I. Shirshov, On bases of free Lie algebras, Algebra i Logika 1 (1) (1962) 14-19.

[32] A.I. Shirshov, Some algorithmic problems for ϵ-algebras, Sibirsk. Mat. Zh. 3 (1) (1962) 132-137.

[33] A.I. Shirshov, Some algorithmic problems for Lie algebras, Sibirsk. Mat. Zh. 3 (2) (1962) 292-296.

[34] Selected works of A.I. Shirshov. Eds: L.A. Bokut, V. Latyshev, I. Shestakov, E. Zelmanov, Trs. M. Bremner and M. Kotchetov. Birkhäuser, Basel, Boston, Berlin, vii, P.241 (2009).

[35] Ralph Stöhr, Bases, filtrations and module decompositions of free Lie algebras, J. Pure Appl. Algebra 212 (5) (2008) 1187-1206.

[36] V.A. Ufnarovskij, Combinatorial and asymptotic methods in algebra, Algebra, VI, 1-196, Encyclopedia Math. Sci., 57, Springer, Berlin, 1995.

[37] G. Viennot, Une generalization des ensembles de Hall, C.R. Acad. Sci. Paris Ser. A 276 (1973) 599-602.

[38] G. Viennot, Algebras de Lie libres et monoid libres. Bases des Lie algebres et facrorizations des monoides libres. Lecture Notes in Mathematics, 691. Berlin, Heidelberg, New York, Springer-Verlag, 124 p. (1978).

[39] E. Zelmanov, Nil rings and periodic groups, KMS Lecture Notes in Mathematics. Seoul: Korean Mathematical Society, x, 79 p. (1992).